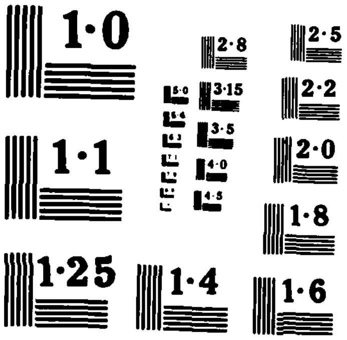
AD-A158 083 TACFIRE ERROR CONTROL: IMPROVEMENTS USING ITERATED CODES(U) ARMY BALLISTIC RESEARCH LAB ABERDEEN PROVING GROUND MD A B COOPER JUN 85 BRL-MR-3453 1/1

UNCLASSIFIED F/G 17/2 NL

END

FILMED

DTIC



NATIONAL BUREAU OF STANDARDS
MICROCOPY RESOLUTION TEST CHART

2

AD

US ARMY
MATERIEL
COMMAND

MEMORANDUM REPORT BRL-MR-3453

TACFIRE ERROR CONTROL: IMPROVEMENTS USING ITERATED CODES

A. Brinton Cooper, III

June 1985

US ARMY BALLISTIC RESEARCH LABORATORY
ABERDEEN PROVING GROUND, MARYLAND

Destroy this report when it is no longer needed.
Do not return it to the originator.

Additional copies of this report may be obtained from the National Technical Information Service, U. S. Department of Commerce, Springfield, Virginia 22161.

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

The use of trade names or manufacturers' names in this report does not constitute indorsement of any commercial product.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
MEMORANDUM REPORT BRL MR- 3453

2. GOVT ACCESSION NO.
AD-A158083

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
TACFIRE ERROR CONTROL: IMPROVEMENTS USING ITERATED CODES

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
A. BRINTON COOPER, III

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army Ballistic Research Laboratory
ATTN: AMXBR-SECAD
Aberdeen Proving Ground, MD 21005-5066

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
1L161102AH43

11. CONTROLLING OFFICE NAME AND ADDRESS
US Army Ballistic Research Laboratory
ATTN: AMXBR-OD-ST
Aberdeen Proving Ground, MD 21005-5066

12. REPORT DATE
June 1985

13. NUMBER OF PAGES
28

14. MONITORING AGENCY NAME & ADDRESS(If different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
N/A

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES
This report supersedes IMR No 799, 800 (dated Dec 83) and part of IMR 817 (dated Jun 84).

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Error Control Coding
Iterated Codes
Error Probability

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

TACFIRE applies a shortened Hamming code to each character of a message. The correction of a single bit error within an encoded character is made by the Hamming decoder. Detectable but not correctable error patterns include all of two and many of four, six, eight, and 10 errors and cause rejection (non-acknowledgment)of the message. On noisy communication channels, retransmissions of rejected messages consume significant resources. To mitigate this high channel usage, a second stage of coding is applied to the characters of the
(continued on reverse side)

more

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Item 20. ABSTRACT (cont'd)

message considered as an information set. This use of Reed-Solomon codes is shown to reduce the rate of message rejection for certain noisy channels.

Additional keywords: tactical communications, message processing, iterations

TABLE OF CONTENT

LIST OF ILLUSTRATIONS

Page

LIST OF TABLES

Page

I. INTRODUCTION

Modern battlefield data communications is often accomplished by formatting digital information into messages composed of characters from a predefined alphabet having finite size. A message *header* is prepended to the message and contains source, destination, precedence, type, and other overhead information.

Because users of military communications require that message delivery be reliable and error-free, certain additional message processing operations are performed at both source and destination. Typically, certain numbers are computed as functions of the message content and are appended to the message. These numbers are recomputed at the destination and compared with the respective received values. If they agree, the recipient acknowledges receipt by sending a short message to the source. Otherwise, in some systems a "non-acknowledgement" message is sent; in others, the destination simply remains silent. In this manner, the sender knows if the message was accepted by the destination. If a transmitted message is not acknowledged within a reasonable time, the sender usually retransmits it.

While such retransmission protocols can provide nearly certain assurance of the receipt of correct messages, poor channel conditions and heavy message traffic will severely load the communication channels with retransmitted messages and their acknowledgements. This often results in unacceptable delays. The problem is compounded when acknowledgement messages themselves are aborted in the same manner, causing a retransmission of the original message. Suggested improvements have included transmitting each message twice (or more) and eliminating acknowledgement messages. This suggestion probably will not play well in Peoria as the military are not likely to give up the assurance which they feel is provided by positive acknowledgement.

This report postulates typical situations and evaluates them quantitatively. The main contribution is the demonstration of an additional error control scheme which could be used on top of the existing algorithms. A nonbinary Reed-Solomon (RS) code is used to demonstrate the principle. It treats each detected character error as an "erasure" in which the location of the erroneous character is known but where the value transmitted is not. Since decoders for error control codes not only correct received symbol errors but also fill in symbols which the channel has erased, the two-tier scheme suggests that improvements may be possible.

II. BIT ERROR CONTROL IN MESSAGE COMMUNICATIONS

A. THE PROTOCOLS

The simplest of communication protocols computes, for the entire message, a single "checksum" [TANE81]. If the checksum computed by the recipient does not agree with that appended to the received message, the latter is discarded and must be retransmitted.

A more powerful retransmission scheme uses an error control code with modest error correction capabilities and the ability to detect somewhat more severe error patterns. It corrects some channel-induced errors and indicates the existence of others. Such an error detection condition causes the datalink protocol [TANE81] to suppress acknowledgement of the message. After a timeout period, the source of the unacknowledged message will retransmit it.

High levels of noise or interference in a channel will result in the need for multiple transmissions of a significant fraction of all messages in order to guarantee successful receipt.

In what follows, the performance of the error control method used in the TACFIRE fire direction system is determined for a range of communication channels, and additional processing is examined and shown to provide significant improvement for modest changes in hardware.

B. LINEAR BLOCK CODES

Binary information which naturally occurs in fixed size blocks or which can be conveniently partitioned into such blocks lends itself to error control using linear block codes (LBC). Mathematically, a LBC is a k-dimensional subspace of the vector space of n-tuples over the finite field, $GF(q^k)$, of q^k elements, where q is a positive integer power of a prime and k is any positive integer.

Structurally, to each block of k information bits from the source, are appended $(n - k)$ redundant bits, each computed as a linear combination of some subset of the information bits. That is, they transmit no additional information but represent a form of controlled redundancy. Each information bit must be included in the computation of at least one redundant bit. We assume throughout that all 2^k information patterns are equally likely. Hence, the encoded source can produce any of 2^k binary n-tuples. It is said that each redundant bit is a parity check [LIN&83] on the information bits which constitute its sum. The value of k is known as the *dimension* of the code; its *block length* is n.

At the destination, the n-tuples (some of whose positions may have been changed by channel noise) are presented to a decoder which may do some or all of the following:

1. It may recompute, from the information positions, the parity check bits. If they are the same as those received, it decides that the codeword was received without error.

2. If the computed parity bits differ from those received, it can execute an algorithm to attempt to locate which codeword positions were modified by channel noise and correct those positions.

3. If the decoder cannot determine the error locations, it can signal same to the message recipient.

Figure 1.1 shows a model of the process by which information is conveyed from a binary source (*e.g.*, a message composition device) over a channel to a destination using a LBC.

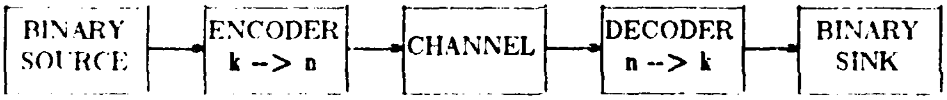


Figure 1.1 Binary Model for Linear Block Codes

Rules for selecting the subsets of information digits to be checked by a parity digit are constructed so as to make the codewords pairwise as different as possible. If they are as different as possible, correct decoding can often be unambiguously accomplished by selecting as the transmitted codeword that which is "nearest" to the received n-tuple. Thus, while encoding produces a unique n-tuple for every block of k information digits, decoding must map many n-tuples into a single k-tuple

Complete treatments of LBC can be found in [PETE72] and [LIN&83].

C. THE BINARY SYMMETRIC CHANNEL

The binary symmetric channel BSC(p) induces errors in binary symbols independently with probability p. It is shown in Figure 2.1 as the addition, to the transmitted data, of the output of a random binary symbol generator which produces a binary ONE with probability p and a ZERO with probability $(1 - p)$. Thus, an information bit will be inverted if and only if the noise bit is a

ONE, and we say that the channel bit error probability is p. Information theoretic considerations demand that $p < 0.5$ [GALL68].

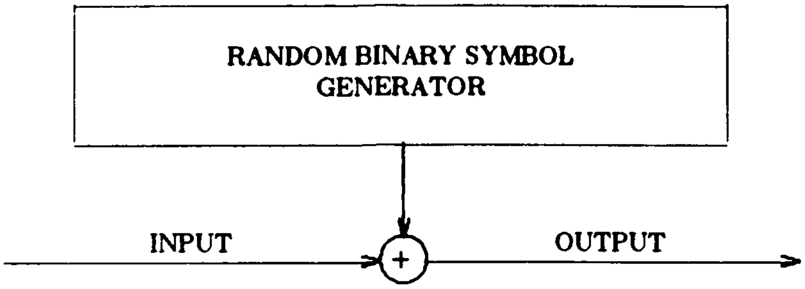


Figure 2.1 The Binary Symmetric Channel

The behavior of BSC(p) is further represented by the state transition diagram of Figure 2.2.

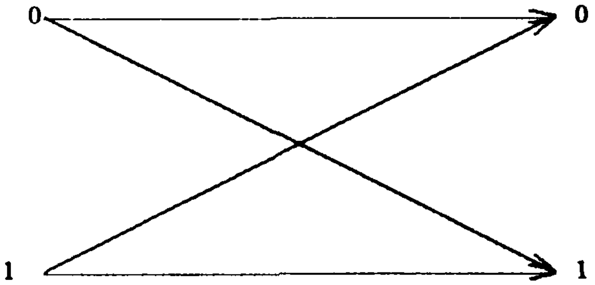


Figure 2.2 State Transitions in The Binary Symmetric Channel

The BSC provides a convenient vehicle for comparing error detection and correction techniques. Many physical channels can be modeled as BSC(p) provided suitable techniques such as interleaving are used.

D. HAMMING CODES AND SHORTENED HAMMING CODES

One aim of code design is to make the codewords as different as possible so that, when corrupted by channel noise, a received word tends to be nearer the word transmitted than to any other word. For transmission over BSC(p), code word difference is expressed as Hamming distance: the number of positions in which the two words differ. It can be shown [PETE72] that the minimum distance d between two words over a given code guarantees that the code can correct any error pattern of t or fewer errors provided

$$t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

where the $\lfloor \cdot \rfloor$ notation indicates the integer part of the argument. For linear block codes, the minimum distance between two codewords is equal to the Hamming weight (number of non-zero positions) of the minimum weight, non-zero codeword.

Detailed structure of the codewords can be encapsulated in a (k x n) code generator matrix, G. A binary k-tuple is encoded by postmultiplying it by G to produce a length n codeword.

Hence, all codewords are linear combinations of the rows of G. Each linear code

$$(v_1, v_2, \cdots v_n) = (a_1, a_2, \cdots a_k)G \tag{2-1}$$

also has an associated parity check matrix, H, with the property that the product of any codeword with the transpose of H gives the zero vector:

$$vH^T = 0 \tag{2-2}$$

The relation between H and G can be seen by ordering the columns of H so that it assumes the form:

$$H = [Q \mid I_{n-k}] \tag{2-3}$$

The orthogonality property of (2-2) then causes the code generator to have the form [LIN&83]

$$G = [I_k \mid Q^T] \tag{2-4}$$

where I_j is the jth order identity matrix and T indicates matrix transposition.

Hamming codes [HAMM50] are block codes having the capability to correct exactly one error per codeword. If an additional parity check is computed on the entire codeword, the Hamming decoder can detect any combination of two errors in a received word as well.

Codewords have length and dimension as shown in (2-5). All the non-zero m-tuples are the columns of the code's parity check matrix.

$$\begin{aligned} n &= 2^m - 1 \\ k &= n - m \end{aligned} \tag{2-5}$$

Thus, there is one Hamming code for each value of m.

The (15,11) single error correcting Hamming code has the parity check matrix, (2-6), produced by writing as columns all the binary 4-tuples, ordered numerically.

$$H = \begin{bmatrix} 000000011111111 \\ 000111100001111 \\ 011001100110011 \\ 101010101010101 \end{bmatrix} \tag{2-6}$$

To obtain the generator matrix of this code, the columns of the parity check matrix are reordered according to (2-3):

$$H1 = \begin{bmatrix} 000011111111000 \\ 011100011110100 \\ 101101100110010 \\ 110110101010001 \end{bmatrix} \tag{2-7}$$

An augmented generator matrix, then, can be written according to (2-4) as:

$$G = \begin{bmatrix} 1000000000000111 \\ 0100000000001011 \\ 0010000000001101 \\ 0001000000001110 \\ 0000100000010011 \\ 0000010000010101 \\ 0000001000010110 \\ 0000000100011001 \\ 0000000010011010 \\ 0000000001011100 \\ 0000000000111111 \end{bmatrix} \tag{2-8}$$

The 16th column, an even parity check on the entire row, has been added for double error detection. See Section E, below.

Any error control code of length n can be shortened to length $(n-s)$ by setting to zero s positions in the information vector. If the first s positions are those set to zero, then all codewords will begin with s zeros which need not be transmitted. This results in a code of length $(n-s)$ and dimension $(k-s)$. For example, to construct the TACFIRE DMD error control code, one shortens the (16,11) code of (2-8) by setting the first four information positions to zero, resulting in the (12,7) shortened Hamming code of (2-9).

$$G = \begin{bmatrix} 100000010011 \\ 010000010101 \\ 001000010110 \\ 000100011001 \\ 000010011010 \\ 000001011100 \\ 000000111111 \end{bmatrix} \tag{2-9}$$

E. PERFORMANCE OF (12,7) SHORTENED HAMMING CODE ON BSC(p)

It is useful to demonstrate the performance of this code on the binary symmetric channel at this point as the results will be needed later.

According to the TACFIRE datalink protocol [TACF80], the occurrence of two bit errors in one character, which causes an error detection condition, prevents acknowledgement of receipt of the message; therefore, the source perceives failure of message receipt and retransmits the message. The probability of such an event is given by (2-10) which is an underbound to the actual detected error probability since some patterns of 4, 6, 8, and 10 errors can be detected by the decoder.

$$P_2 = \binom{12}{2} \; p^2 \; (1-p)^{12-2} \tag{2-10}$$

Two conditions are necessary for a Hamming decoder to detect the presence of an uncorrectable error pattern:

a. The received vector does not belong to the code. This is checked by a simple matrix multiplication or the evaluation of five or fewer linear equations with binary coefficients.

b. The received vector has even parity. The decoder can correct no error pattern of even weight as the code can correct only single errors.

However, those even weight error patterns which map the transmitted codeword into another codeword are undetectable. The number of such patterns is given by the *weight*

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. BRL Report Number ______________________________ Date of Report _____________

2. Date Report Received ____

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) ____________________

____

____

4. How specifically, is the report being used? (Information source, design data, procedure, source of ideas, etc.) ____

____

____

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided or efficiencies achieved, etc? If so, please elaborate. ____

____

____

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.)

____

____

____

CURRENT ADDRESS

____
Name

____
Organization

____
Address

____
City, State, Zip

7. If indicating a Change of Address or Address Correction, please provide the New or Correct Address in Block 6 above and the Old or Incorrect address below.

OLD ADDRESS

____
Name

____
Organization

____
Address

____
City, State, Zip

(Remove this sheet along the perforation, fold as indicated, staple or tape closed, and mail.)

DISTRIBUTION LIST

Aberdeen Proving Ground

Commander, USATECOM
ATTN: AMSTE-CM-F
AMSTE-AD-A
AMSTE-AD-I
AMSTE-AD-S
AMSTE-TO-F
AMSTE-CT-C

Dir, USAHEL
ATTN: AMXHE-D
AMXHE-FT
AMXHE-CS
AMXHE-CC
AMXHE-SP
AMXHE-FS (Library)

Dir, USAMSAA
ATTN: AMXSY-D
AMXSY-G
AMXSY-GI
AMXSY-GS
AMXSY-GA
AMXSY-C
Mr Fox
Mr Chizmar
Ms Stratton
Mr Ward
Ms Randall
Ms Dumer
AMXSY-R
AMXSY-MP, H. Cohen

Cdr, CRDC, AMCCOM
ATTN: SMCCR-RSP-A
SMCCR-MU
SMCCR-SPS-IL

DISTRIBUTION LIST

No. of Copies — Organization

1 Commander
US Army Signal Center & School
ATTN: ATZH
Fort Gordon, GA 30905

1 Commander
US Army Development & Employment Agency
ATTN: MODE-TED-SAB
Fort Lewis, WA 98433

1 Chair, Department of Mathematics
US Military Academy
West Point, NY 10996

1 Chair, Department of Mathematics
US Naval Academy
Annapolis, MD 21402

1 US Air Force Academy
Chair, Department of Mathematics
Colorado Springs, CO 80901

1 Commander
Naval Surface Weapons Center
ATTN: Technical Director
Silver Spring, MD 20910

1 Commander
Naval Surface Weapons Center
Weapons Laboratory
ATTN: Technical Director
Dahlgren, VA 22448

1 Chief, Ground Operations Div
Development Center
Marine Corps Development and Education Command
Quantico, VA 22134

No. of Copies — Organization

1 Office Chief (at Navy A.I.)
Navy Research Laboratories
ATTN: Jude Franklin
Code 7510
Washington, DC 20375

1 AFWL/SUL
Kirtland AFB, NM 87117

1 Magnavox Electronics Systems Co.
Tactical Systems
ATTN: D. Willis
1313 Production Road
Ft. Wayne, IN 46808

1 Singer Librascope
ATTN: T.B. Aitken
833 Sonora Avenue
Glendale, CA 91201

1 Litton Data Systems
8000 Woodley Avenue
VanNuys, CA 91406

1 Norden Systems, Inc
Norden Place
Norwalk, CT 06855

1 Commander
Naval Research Laboratory
Code 7521, Dr. J. Wieselthier
Washington, DC 20375

1 Air Force Armament Laboratory
ATTN: AFATL/DLODL
Eglin AFB, FL 32542-5000

DISTRIBUTION LIST

No. of Copies Organization

1 Project Manager
Position Location Reporting
System/Tactical Information
Distributing System
ATTN: AMCPM-PL
Fort Monmouth, NJ 07703

1 Project Manager
Remotely Piloted Vehicle
ATTN: AMCPM-RPV
4300 Goodfellow Blvd
St. Louis, MO 63120

1 Project Manager
Single Channel Ground &
Airborne Radio System
ATTN: AMCPM-GARS
Fort Monmouth, NJ 07703

1 Project Manager, TACFIRE/Field
Artillery Tactical Data Sys
ATTN: DRCPM-TF
Fort Monmouth, NJ 07703

1 Project Manager, TACFIRE
Software Support Group
ATTN: AMCPM-TF-FS
Fort Sill, OK 73503

1 Commander
US Army Combined Arms Center -
Ft. Leavenworth
ATTN: ATOR-C
Fort Leavenworth, KS 66027-5080

1 Commander
US Army Combat Developments
Experimentation Command
ATTN: ATEC
Fort Ord, CA 93941

No. of Copies Organization

1 Director
US Army TRADOC Systems
Analysis Activity
ATTN: ATAA-SL
White Sands Missile Range
NM 88002

1 President
US Army Artillery Board
ATTN: ATZR-BD
Fort Sill, OK 73503

1 Commandant
US Army Infantry School
ATTN: ATSH-CD-CSO-OR
Fort Benning, GA 31905-5400

1 Commandant
US Army Armor School
ATTN: ATSB-CD
Fort Knox, KY 40121

1 Commander
US Army Field Artillery Center
and School
ATTN: ATZR
Ft. Sill, OK 73503

1 Commander
US Army Field Artillery Center
and School
ATTN: ATSF-TSM-TF
Fort Sill, OK 73503

2 Commander
US Army Field Artillery Center
and School
ATTN: ATSF-TSM-MLRS
ATSF-TSM-RPV
Fort Sill, OK 73503

1 Commandant
US Army Intelligence Center
and School
ATTN: ATSI
Fort Huachuca, AZ 85613

DISTRIBUTION LIST

No. of Copies — Organization

3 Commander
US Army Harry Diamond Labs.
ATTN: DELHD
DELHD-TD, Dr. Scully
DELHD-NW-EMB
2800 Powder Mill Road
Adelphi, MD 20783

1 Director
Night Vision Laboratory
ATTN: AMLNV
Fort Belvoir, VA 22060

1 Director
US Army Signals Warfare Laboratory
ATTN: AMLSW
Vint Hill Farms Station
Warrenton, VA 22186

1 Commander
US Army Engineer and Topographic Laboratories
ATTN: ETL
Fort Belvoir, VA 22060

2 Commander
US Army Research Office
ATTN: Dr. Suttle
Dr. Chandra
Box 12211
Research Triangle Park, NC 27709-2211

1 Commander
US Army Research, Development and Standardization Group
Australia
APO SF 96404

No. of Copies — Organization

1 Commander
US Army Research, Development, and Standardization Group
Canada
National Defence HQs
Elgin St
Ottawa K1A OK2 Ontario
Canada

1 Commander
US Army Research, Development and Standardization Group
United Kingdom
USARDSG (UK) Box 65
FPO New York 09510

1 Project Manager
Control and Analysis Center
ATTN: AMCPM-CAC
Vint Hill Farms Station
Warrenton, VA 22186

1 Project Manager
HELLFIRE/GLD
Redstone Arsenal, AL 35898

1 Project Manager
Air Defense Command and Control Systems
ATTN: AMCPM-ADCC
Redstone Arsenal, AL 35898

1 Project Manager
Joint Tactical Missile System
ATTN: AMCPM-JTACMS
Redstone Arsenal, AL 35898

1 Project Manager
Multiple Launch Rocket System
ATTN: AMCPM-RS
Redstone Arsenal, AL 35898

1 Project Manager
Operations Tactical Data Systems
ATTN: AMCPM-OPTADS
Fort Monmouth, NJ 07703

DISTRIBUTION LIST

No. of Copies — Organization

1 Commander
US Army Aviation Research
and Development Command
ATTN: AMSAV-E
4300 Goodfellow Boulevard
St. Louis, MO 63120

1 Director
US Army Air Mobility Research
and Development Laboratory
Ames Research Center
Moffett Field, CA 94035

2 Commander
ERADCOM HQ
ATTN: AMDEL
AMDEL (VISTA)
3800 Powder Mill Road
Adelphi, MD 20783

1 Commander
US Army Communications -
Electronics Command
ATTN: AMSEL-ED
Fort Monmouth, NJ 07703

4 Commander
US Army CECOM
ATTN: AMDCO-COM-D, Dr. Dworkin
AMDCO-COM-RF
AMDCO-COM-RN
AMDCO-COM-RX
Fort Monmouth, NJ 07703

4 Commander
US Army CECOM
ATTN: AMDCO-SEI-A
AMDCO-SEI-E
AMDCO-SEI-I
AMDCO-TCS
Fort Monmouth, NJ 07703

1 Commander
US Army Electronics Research
and Development Command
Technical Support Activity
ATTN: DELSD-L
Fort Monmouth, NJ 07703

No. of Copies — Organization

1 Commander
US Army Avionics Research and
Development Activity
ATTN: DAVAA
Fort Monmouth, NJ 07703

2 Commander
US Army Electronics Research
and Development Command
Technical Support Activity
ATTN: AMDET-ID
Fort Monmouth, NJ 07703

1 Commander
USA Atmospheric Sciences Lab
ATTN: AMLAS
White Sands Missile Range, NM
88002

1 Commander
US Army Missile Command
ATTN: AMSMI-R
Redstone Arsenal, AL 35898-5630

1 Commander
US Army Missile Command
ATTN: AMSMI-YDL
Redstone Arsenal, AL 35898-5630

1 Commander
US Army Tank Automotive Command
ATTN: AMSTA-TSL
Warren, MI 48090

1 AFELM, The Rand Corporation
ATTN: Library-D
1700 Main Street
Santa Monica, CA 90406

1 Director
Electronic Warfare Laboratory
ATTN: AMLEW
Fort Monmouth, NJ 07703

DISTRIBUTION LIST

No. of Copies Organization

12 Administrator
Defense Technical Info Center
ATTN: DTIC-DDA
Cameron Station
Alexandria, VA 22304-6145

2 Director
DARPA
ATTN: Info Processing
Techniques Office
1400 Wilson Boulevard
Arlington, VA 22209

1 Director
DARPA
ATTN: Tactical Technology Ofc
1400 Wilson Boulevard
Arlington, VA 22209

1 HQDA
DAMA-ART-M
Washington, DC 20310

1 HQDA (DAMA-ARR)
ATTN: Dr. Verderame
Washington, DC 20310-0622

1 Commander
US Army Materiel Command
ATTN: AMCDRA-ST
5001 Eisenhower Avenue
Alexandria, VA 22333-0001

1 Commander
US Army Materiel Command
ATTN: AMCLD
5001 Eisenhower Avenue
Alexandria, VA 23333

1 Commander
US Army Materiel Command
ATTN: AMCDE-SC
5001 Eisenhower Avenue
Alexandria, VA 23333

No. of Copies Organization

1 Commander
US Army Materiel Command
ATTN: AMCDE-SB
5001 Eisenhower Avenue
Alexandria, VA 23333

1 Commander
US Army Materiel Command
ATTN: AMCDE-SG
5001 Eisenhower Avenue
Alexandria, VA 23333

1 New Thrust Demo Manager
New Thrust Management Office
ATTN: AMCLD-ST
8330 Old Courthouse Road
Vienna, VA 22180

1 Commander
Armament R&D Center
US Army AMCCOM
ATTN: SMCAR-TDC
Dover, NJ 07801-5001

1 Commander
Armament R&D Center
US Army AMCCOM
ATTN: SMCAR-TSS
Dover, NJ 07801-5001

1 Commander
US Army Armament, Munitions &
Chemical Command
ATTN: SMCAR-ESP-L
Rock Island, IL 61299-6000

1 Director
Benet Weapons Laboratory
Armament R&D Center
US Army AMCCOM
ATTN: SMCAR-LCB-TL
Watervliet, NY 12189

REFERENCES

[TANE81] Tanenbaum, A. S., *Computer Networks,* Prentice-Hall, Englewood Cliffs, 1981.

[LIN&83] Lin, S. and D. J. Costello, Jr, *Error Control Coding: Fundamentals and Limitations,* Prentice-Hall, Inc., Englewood Cliffs, 1983.

[PETE72] Peterson, W. W. and E. J. Weldon, Jr., *Error Correcting Codes,* MIT Press, Cambridge, 1972.

[GALL68] Gallager, R. G., *Information Theory and Reliable Communications,* Wiley, New York, 1968.

[HAMM50] Hamming, R. W., "Error Detecting and Error Correcting Codes," *BSTJ,* vol XXVI, 1950.

[TACF80] EL-SS-2603, *Prime Item Specification for Digital Message Device AN/PSG-2A,* 31 January 1980.

[COOP78] Cooper, A. Brinton, III, "Algebraic Codes Constructed from other Algebraic Codes: A Short Survey and some Recent Results," in *Communication Systems and Random Process Theory,* Sijthoff & Noordhoff, 1978 The Netherlands.

[GORE73] Gore, W. C., "Transmitting Binary Symbols with Reed-Solomon Codes," 1973 Princeton Conference on Information Sciences and Systems.

[BERL68] Berlekamp, Elwyn R., *Algebraic Coding Theory,* McGraw-Hill, New York, 1968.

[REED60] Reed, I. S. and G. Solomon, "Polynomial Codes over certain Finite Fields," *J. SIAM,* v8, June 1960.

[BLAH79] Blahut, R. E., "Transform Techniques for Error Control Codes," *IBM. J. R&D,* v23, No 3, May 1979.

[FARR79] Farrell, P.G., "Soft Decision Techniques," in *Algebraic Coding Theory and Applications,* G. Longo ed., Springer-Verlag, New York, 1979.

[FORN66] Forney, G. D. *Concatenated Codes,* MIT Press, Cambridge, 1966.

discrete when, in fact, it is not. Such channel models are realized in practice by examining the received waveform (signal + noise) and making a statistical decision as to whether a binary 0 or a 1 was received. In the process, information about the reliability of that decision is discarded. To use that information in order to improve character and message reception reliability, "soft decision" detection and decoding techniques [FARR79] are under investigation. Significant improvements in message communication havc been claimed for these methods, and they should be investigated.

Finally, the Hamming and RS codes were chosen for this part of the investigation because of their use in TACFIRE and their popularity among coding theorists and communication system designers, respectively. The technique studied above is related to "concatenated codes" [FORN66] which can be constructed from a variety of sets of constituent codes [COOP78]. Research is needed to select, for this application, codes which are optimum in terms of performance vs decoding complexity.

p	P_{ce}	P_{de}
0.10	0.2502	0.5207
0.08	0.1835	0.1029
0.07	0.1565	0.0307
0.06	0.1279	$4.94 \text{ x } 10^{-3}$
0.05	0.09879	$3.21 \text{ x } 10^{-4}$
0.04	0.07206	$5.25 \text{ x } 10^{-6}$
0.03	0.04380	$9.36 \text{ x } 10^{-9}$
0.02	0.02157	$3.09 \text{ x } 10^{-13}$
0.01	$5.968 \text{ x } 10^{-3}$	$7.30 \text{ x } 10^{-22}$
$8.0 \text{ x } 10^{-3}$	$3.968 \text{ x } 10^{-3}$	$8.72 \text{ x } 10^{-25}$
$6.0 \text{ x } 10^{-3}$	$2.237 \text{ x } 10^{-3}$	$1.30 \text{ x } 10^{-28}$
$5.0 \text{ x } 10^{-3}$	$1.569 \text{ x } 10^{-3}$	$4.61 \text{ x } 10^{-31}$
$4.0 \text{ x } 10^{-3}$	$1.015 \text{ x } 10^{-3}$	$4.45 \text{ x } 10^{-34}$
$3.0 \text{ x } 10^{-3}$	$5.764 \text{ x } 10^{-4}$	$5.29 \text{ x } 10^{-38}$

Table 3.1 Probability of Decoding Failure for RS Codes.

IV CONCLUSIONS

A. DISCUSSION OF RESULTS

Improvement of the message rejection rate by several orders of magnitude has been demonstrated. The present TACFIRE coding technique employs only the shortened Hamming code; when used on channels with coherent frequency shift keying (FSK) (a common method of impressing digital information onto FM radio signals) with values of signal to noise ratio of approximately 4 to 8 dB, it produced message rejection rates ranging from $6 x 10^{-4}$ to 0.1. With the concatenation of RS codes, these rates dropped to a range of $5 x 10^{-38}$ to $4 x 10^{-4}$.

The penalty to be paid for this improvement is twofold. First, messages have been lengthened from 48 to 63 characters, an increase of 31% with no corresponding increase in the amount of information transmitted. Second, an additional stage of encoding and, more significantly, of decoding must be added. While many efficient decoding algorithms for RS codes are known, [BERL68, BLAH79], the evaluation of the added complexity must be the subject of another report.

B. FURTHER WORK

Undetectable error patterns are more insidious than those considered in this note. For example, 38 error patterns of weight four are codewords. Since the sum of two codewords is a codeword, the received vector will be one also. In such cases, no error condition can be detected. This behavior will be examined in a forthcoming report.

In addition to determining the impact of adding RS decoders to existing TACFIRE message processing, other factors must be studied. Better coding schemes for new Army Field Artillery Tactical Data Systems (AFATDS) equpiment should be investigated.

For this analysis, BSC(p) was used with values of p from 0.003 to 0.4. As asserted, the BSC is a valid model for certain channels which are limited by the noise generated in the radio frequency amplifiers of the receiver. Conditions under which such a model is valid must be determined. Further, more realistic noise and interference models (*e.g.*, noise bursts) must be considered, and coding techniques such as the one studied here must be evaluated against them.

Another consideration is that such channel models as the BSC assume that the world is

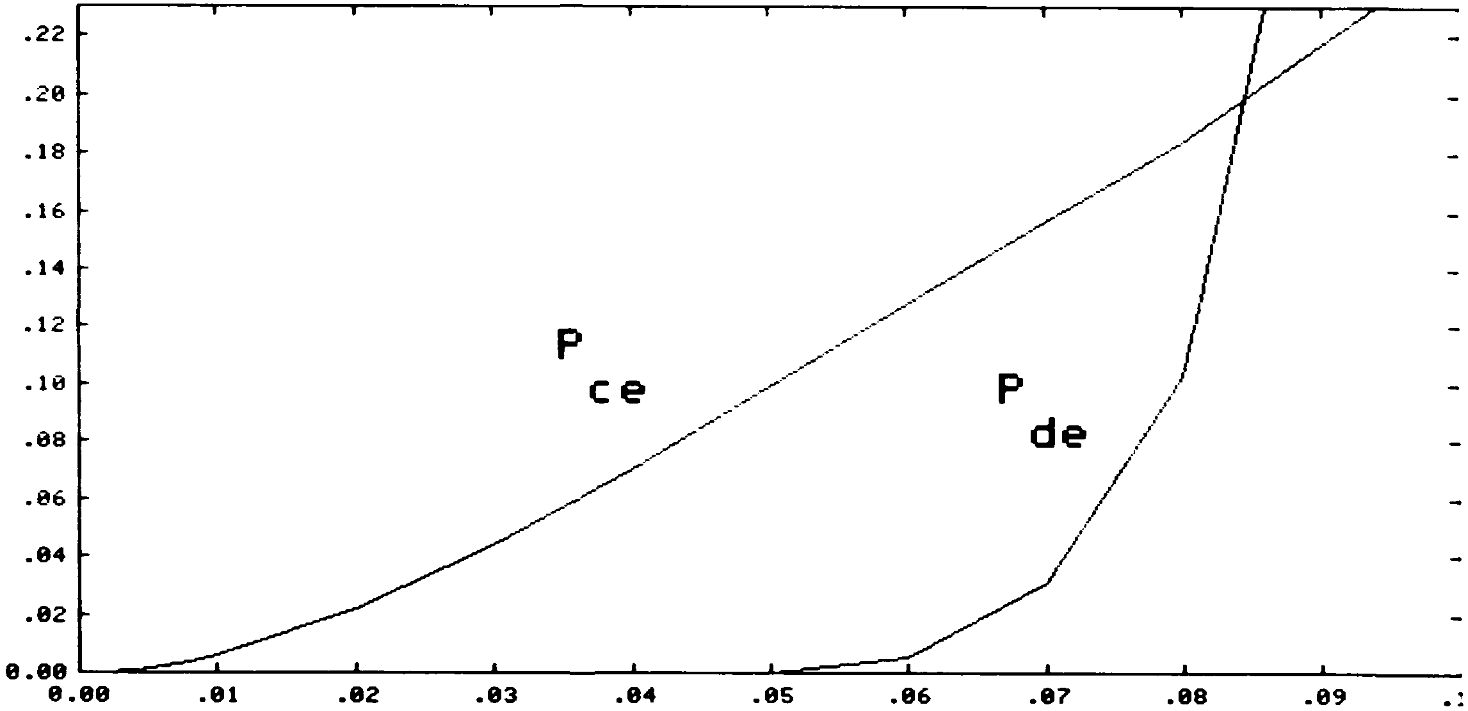


Figure 3.1. Character Error Detection and RS decoding Failure Probabilities

distance $d = n - k + 1$ [REED60]. For a suitable choice of m, we will select a RS code for use on the erasure channel previously described.

D. PERFORMANCE OF THE COMBINED CODING SCHEME

Before actually computing the performance of this coding scheme, its mappings will be carefully presented. A specific example, the TACFIRE Digital Message Device (DMD) format, will be used.

The DMD character set is a 49-element subset of full 7-bit ASCII. Each character is formed according to the standard 7-bit patterns. However, since 49 < 64, only 6 bits are actually needed in order to have a unique binary pattern for each symbol to be transmitted—a fact which we shall now use.

As the DMD produces 7-bit ASCII characters, they are encoded by the (12,7) Hamming encoder as at present. Simultaneously, however, these 7 bit characters are mapped into 6-bit patterns. When 48 of these (the length of a DMD message) have been buffered, 15 parity check characters will be computed on them according to the generator matrix of a (63,48) Reed-Solomon code over GF(2^6). These parity check symbols are, of course, binary 6-tuples. These 6-tuples will be mapped back into binary 7-tuples according to the inverse of the 7 to 6 mapping. (A rule or a table can be used, so long as the transformation is reversible.) These 15 7-bit characters are now encoded by the (12,7) Hamming encoder and are concatenated with the 48 message characters previously encoded.

Decoding is accomplished in two stages. Received information is processed first by the decoder for the (12,7) Hamming code. Any double weight error pattern will force this decoder to output an "erasure" condition. Correctly decoded characters are presented as binary 7-tuples. These are converted to 6-tuples using the same map as at the encoder and are presented to the decoder for the (63,48) RS code.

Since character erasures are easily sensed by the RS decoder, it should not try to decode when more than 15 erasures have occurred. In the context of this note, the received message should not be acknowledged. The probability that a received message is not acknowledged is, therefore,

$$P_{de} = \sum_{j=16}^{63} \binom{63}{j} P_{ce}^{j} (1-P_{ce})^{63-j} \tag{3-2}$$

where P_{ce} is the probability of a character erasure at the output of the Hamming decoder. Values of P_{ce} for the BSC are obtained from Table 2.1 and the final results are shown in Table 3.1 and plotted in Figure 3.1.

Table 2.2 shows the detected character error probability (and, hence, the probability of a non-acknowledged message) as a function of the channel bit error probability for values of the latter from 0.003 to 0.40. These data are plotted in Figure 3.1.

III. ERASURE CHANNELS AND REED-SOLOMON CODES

A. INTRODUCTION

An iteration of encoding and decoding can be added to the scheme so far described. Essentially, the output of the original encoder can be further encoded according to the rules for another suitably chosen error correcting code. At the channel output, the original code can first be decoded as before and the result submitted to a second decoder for further processing [COOP78]. It is useful to postulate a different kind of channel when introducing the additional coding.

B. THE ERASURE CHANNEL

In a received message, a character position where a detectable but uncorrectable error pattern has occurred in the channel can be considered as an *erasure, i.e.,* a location where the decoder knows that an error pattern has occurred which it cannot correct. Linear block codes can handle erasures more handily than they can handle errors whose positions are unknown. For example, a code with minimum distance d can correct (fill in) e erasures in a received word where

$$d \geq e + 1 \tag{3-1a}$$

whereas

$$d \geq 2t + 1 \tag{3-1b}$$

where $t =$ the number of errors correctable by the same code.

We now take a modified viewpoint and consider a noisy channel transmitting characters (binary m-tuples) rather than individual bits [GORE73]. Characters either are received correctly from this channel or they are erased. The probability of a character erasure is the probability of any detectable error pattern. For the (12,7) shortened Hamming code discussed in Section II, this is given by (2-11).

So the channel under consideration accepts characters, each represented by a binary m-tuple, and presents to the destination a character erasure with probability given by (2–11). In what follows, an error detecting and correcting scheme to make this channel quite reliable is described.

C. EXTENSION FIELDS AND THE BINARY SYMMETRIC CHANNEL

If binary symbols are manipulated m at a time, modern algebra permits all the ordinary arithmetic operations (addition, multiplication, inverses, and identities) customarily performed upon real numbers, provided the m-tuples are structured according to certain rules [BERL68]. We say that such a set of elements and operations is a Galois field of 2^m elements, $GF(2^m)$. (When $m = 1$, we have the familiar binary field.) In $GF(2^m)$, we can construct linear block codes as we did in the binary case: to every block of k information symbols from $GF(2^m)$ append $(n-k)$ parity check symbols as linear combinations of the information. Note that this arithmetic is performed in $GF(2^m)$.

An interesting class of codes for these fields is that of the Reed-Solomon (RS) codes, which have the largest minimum distance possible for a given length and dimension (n,k) [BERL68]. A RS code is a linear block code with symbols from $GF(2^m)$, length $n = 2^m - 1$, and minimum *enumerator* for the code: the number of codewords of each weight. Since the shortened (12,7) Hamming code under consideration has only even weight codewords, the probability of a detectable but uncorrectable error pattern is the probability of occurrence, on the binary symmetric channel, of any even weight error pattern which is not a codeword. If the number of codewords of weight i is A_i, this probability is given by (2-11).

$$P_d = \sum_{i=0}^{6}\left[\binom{12}{2i} - A_{2i}\right] p^{2i}\,(1-p)^{(12-2i)} \tag{2-11}$$

The values of A_i can be enumerated by generating all 127 non-zero codewords from the generator matrix given above. They are enumerated in Table 2.1. Values of P_d vs p were computed from (2-11) and are listed in Table 2.2.

i	A_i
0	0
4	38
6	52
8	33
10	4

Table 2.1 Weight Enumerator for the (12,7) Hamming Code.

p	P_d
0.003	5.764 x 10 $^{-4}$
0.004	1.015 x 10 $^{-3}$
0.005	1.569 x 10 $^{-3}$
0.006	2.237 x 10 $^{-3}$
0.008	3.898 x 10 $^{-3}$
0.01	5.968 x 10 $^{-3}$
0.016	0.0144
0.02	0.02157
0.03	0.04380
0.04	0.07206
0.05	0.09879
0.06	0.1279
0.07	0.1565
0.08	0.1835
0.10	0.2502
0.12	0.3000
0.14	0.3415
0.16	0.3749
0.18	0.4011
0.20	0.4212
0.22	0.4357
0.30	0.4634
0.35	0.4675
0.40	0.4684

Table 2.2 Probability of Detected Error Patterns

FOLD HERE

Director
US Army Ballistic Research Laboratory
ATTN: AMXBR-OD-ST
Aberdeen Proving Ground, MD 21005-5066

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO 12062 WASHINGTON,DC

POSTAGE WILL BE PAID BY DEPARTMENT OF THE ARMY

Director
US Army Ballistic Research Laboratory
ATTN: AMXBR-OD-ST
Aberdeen Proving Ground, MD 21005-9989

FOLD HERE